Claims

What is claimed is:

1. A method, comprising:

issuing, via a caller computer, a request to have a firmware service be performed via firmware on a remote computer

authenticating the caller computer; and

performing the firmware service if the caller computer is authenticated, otherwise denying access to the firmware service.

2. The method of claim 1, further comprising initializing a listening mechanism on the remote computer to receive the request.

3. The method of claim 2, wherein the listening mechanism is interrupt-based, further comprising asserting an interrupt on a processor of the remote computer in response to receiving the request.

4. The method of claim 2, wherein the listening mechanism is polling-based, further comprising periodically polling a network interface of the remote computer to determine if the remote computer has received a request.

5. The method of claim 1, wherein the caller computer is authenticated by performing operations including:

issuing an authentication challenge to the caller computer; and

evaluating a response by the caller computer to the authentication challenge.

6. The method of claim 5, wherein the operations further include:

encrypting original data using a first key held by the remote computer to create encrypted original data;

sending the encrypted original data to the calling computer;

decrypting the encrypted original data using a second key held by the caller computer to create decrypted data;

sending the decrypted data back to the remote computer;

comparing the decrypted data with the original data to authenticate the calling computer.

7. The method of claim 6, further comprising extracting the first key from an authentication certificate for the caller computer issued to the remote computer.

8. The method of claim 7, wherein the first key is an public key contained in the authentication certificate and the second key comprises a private key held by the calling computer that is the asymmetric key for the public key.

9. The method of claim 1, further comprising:

issuing at least one authentication certificate to the remote computer, each of said at least one authentication certificate containing authentication information corresponding to a respective caller computer;

receiving authentication credentials from a caller computer;

authenticating the caller computer via the authentication credentials in view of a corresponding authentication certificate from among said at least one authentication certificate issued to the remote computer.

10. The method of claim 9, further comprising determining if an authentication certificate corresponding to the caller computer has expired.

11. The method of claim 9, further comprising determining if an authentication certificate corresponding to the caller computer has been revoked.

12. The method of claim 1, further comprising authenticating the remote computer.

13. The method of claim 1, further comprising sending encrypted traffic relating to the firmware service request and results of the request between the caller computer and the remote computer.

14. The method of claim 13, further comprising performing a cipher negotiation between the caller computer and the remote computer to agree upon an encryption technique used to encrypt and decrypt the encrypted traffic.

15. The method of claim 14, wherein the encryption technique employs at least one session key.

16. The method of claim 1, wherein communications between the caller computer and the remote computer are performed using an out-of-band communication channel that operates independent of an operating system to run or running on the remote computer.

17. An article of manufacture, comprising:

a machine-readable medium on which a plurality of instructions are stored, which when executed perform operations comprising:

receive a request from a caller computer to perform a firmware service;

authenticate the caller computer; and

perform the firmware service if the caller computer is authenticated, otherwise denying access to the firmware service.

18. The article of manufacture of claim 17, wherein execution of the plurality of instructions further performs the operation of initializing a listening mechanism to receive the request.

19. The article of manufacture of claim 17, wherein execution of the plurality of instructions further performs operations including:

issuing an authentication challenge to the caller computer;

receiving a response to the authentication challenge from the caller computer; and

evaluating the response to determine whether the caller computer is authenticate.

20. The article of manufacture of claim 19, wherein evaluating the response to the authentication challenge comprises:

extracting authentication credentials for the caller computer contained in the response;

identifying an authentication certificate corresponding to the caller computer; and

checking authentication credentials for the caller computer against the authentication certificate that is identified.

21. The article of manufacture of claim 20, wherein execution of the plurality of instructions further performs the operation of determining if the authentication certificate that is identified has expired.

22. The article of manufacture of claim 20, wherein execution of the plurality of instructions further performs the operation of determining if the authentication certificate that is identified has been revoked.

23. The article of manufacture of claim 19, wherein execution of the plurality of instructions performs further operations including:

generating a random number;

encrypting the random number using a first key to create an encrypted random number;

sending the encrypted random number to the calling computer;

receiving decrypted data derived from the encrypted random number from the calling computer

comparing the decrypted data with the random number to authenticate the calling computer.

24. The article of manufacture of claim 17, wherein the article comprises a firmware storage device and the plurality of instructions comprise firmware.

25. The article of manufacture of claim 17, wherein execution of the plurality of instructions further performs the operation of performing a cipher negotiation between the caller computer and a remote computer on which the plurality of instructions are executed to agree upon an encryption technique to be used to

encrypt and decrypt encrypted traffic to be sent between the caller computer and the remote computer.

26. The article of manufacture of claim 25, wherein the encryption technique employs a shared asymmetric session key.

27. A computer system, comprising:

a processor;

a memory, operatively coupled to the processor;

a network interface operatively coupled to the processor; and

at least one flash device operatively coupled to the processor on which firmware instructions are stored, which when executed by the processor perform operations comprising:

receive a request to perform a firmware service received from a caller computer via the network interface;

authenticate the caller computer; and

perform the firmware service if the caller computer is authenticated, otherwise denying access to the firmware service

28. The computer system of claim 27, wherein execution of the firmware instructions performs the further operation of periodically polling the network interface to determine if the network interface has received a request from a caller computer to perform a firmware service.

29. The computer system of claim 27, wherein execution of the firmware instructions performs further operations, including:

issuing an authentication challenge to the caller computer;

receiving a response to the authentication challenge from the caller computer; and

evaluating the response to determine whether the caller computer is authenticate.

30. The computer system of claim 27, wherein execution of the firmware instructions further performs the operation of performing a cipher negotiation between the caller computer and the computer system to agree upon an encryption technique to be used to encrypt and decrypt encrypted traffic to be sent between the caller computer and the computer system.